Accompanying this Reply is a Petition for Extension of Time Under 37 CFR 1.136(a) and the required fee.

REMARKS

Claims 1 - 15 remain in the application, and are amended herein.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

Section 101 Rejections

Claims 1 - 15 stand rejected under 35 U.S.C. §101 on the grounds that the claimed invention lacks patentable utility. As mentioned on page 1, second paragraph of the Specification, "Pseudo-random numbers are used for a variety of purposes including simulation studies, information processing, communication, and encryption." Because such processes and devices require random numbers or pseudo-random numbers to function, the generation of pseudo-random numbers is useful and necessary to the utility of such processes and devices. The claimed pseudo-random number generator, by providing pseudo-random numbers that can be used in such processes and devices, necessarily produces a "useful, concrete, and tangible result" in the pseudo-random numbers themselves. (See MPEP, Chapter 2106, Section IV, subsection C, subsection 2, subsection (2)).

The pseudo-random numbers generated by the claimed method and apparatus can be used in a variety of practical applications, including communications systems, encryption processes, digital calibration mechanisms, or other devices which depend upon the availability of random or pseudo-random numbers to properly function. The claims have been amended herein to emphasize that the pseudo-random numbers generated are provided to a storage register from which they can be retrieved, either contemporaneously with generation of the numbers or at a later time, for use in any

device which exploits and capitalizes upon the characteristics of pseudo-random numbers. Thus, the amended claims expressly state a practical application of the generation of pseudo-random numbers, to satisfy the requirements of Section 101. Support for such amendment can be found throughout the Specification, and in particular on page 1, second paragraph.

Claims 1 and 14 stand rejected under 35 U.S.C. §101 on the grounds that they recite manipulating numbers in a fashion that merely represents a mathematical algorithm. Each of those claims, and thus all claims dependant on them, have been amended herein to require that certain elements, and the generated pseudo-random numbers, be stored in a storage register from which the numbers can be provided to devices utilizing pseudo-random numbers. Thus, the method and apparatus of the amended claims is tangible and concrete. Support for such amendment can be found throughout the Specification and in particular in claims 2 and 15, at page 14, line 5, and at page 15, lines 13-14.

Section 112 Rejections

Claims 14 and 15 stand rejected under 35 U.S.C. § 112 as being indefinite for failing to particularly point out and distinctly claim the structure referred to by means plus function language. Each of those claims is amended herein to specifically recite acts for performing each function. Based on supporting language in pages 5 – 17 of the Specification, the amended claims recite that the output matrices initialization means, transition matrices initialization means, offset matrices initialization means, and modulus operator initialization means each function by assigning values to matrix entries or modulus operators, as applicable. Claims 14 and 15 have also been modified to clarify that pseudo-random numbers generated by the claimed apparatus are provided to storage for use in a device that employs pseudo-random numbers.

The Specification specifically points out that:

a.) the output matrices initialization means is any structure which assigns values to matrix entries, including the possibility of obtaining values from a storage register (page 14, lines 5-6 and lines 13-15),

b.) the transition matrices initialization means is any structure which assigns values to the transition matrix entries, including the possibility of assigning values by use of another pseudo-random number generator or by selecting them from a list (page 7, lines 15-20, page 14, line 6-8, and page 15, lines 15-18),

c.) the offset matrices initialization means is any structure which assigns values to matrix entries, including the possibility of assigning values by use of another pseudo-random number generator or by selecting them from a list (page 8, lines 7-11, page 14, lines 8-10, and page 15, lines 18-21),

d.) the modulus operator initialization means is any structure which assigns values to modulus operators, including the possibility of assigning values by use of another pseudo-random number generator or by selecting them from a list (page 9, lines 6-22, page 14, lines 10-12, and page 15, lines 21-24),

e.) the first application means is any structure which utilizes the matrix multiplication operation applying the initial transition matrices to the initial output matrices to create first intermediate matrix values (page 7, lines 2-5, page 14, lines 15-17),

f.) the second application means is any structure which utilizes the matrix addition operation applying the initial offset matrices to the first intermediate matrices to create second intermediate matrix values (page 7, lines 2-6, page 14, lines 15-17),

g.) the third application means is any structure which utilizes modular arithmetic and sequentially applies a set of modulus operators to the second intermediate matrices (page 7, lines 6-7, page 14, lines 17-20) to create values used to update the entries in the output matrices,

h.) the updated output matrices storage means is any structure, including a storage register, which stores updated values of the output matrix entries, (page 14, lines 5-6 and lines 13-15),

i.) the transition matrices updating means is any structure which assigns new values in place of existing transition matrix entries, including the possibility of assigning values by use of another pseudo-random number generator or by selecting them from a list (page 7, lines 15-20, page 14, line 6-8, and page 15, lines 15-18),

j.) the fourth application means is any structure which utilizes the matrix multiplication operation applying the updated transition matrices to the updated output matrices to create updated

first intermediate matrix values (page 7, lines 2-5, page 14, lines 15-17),

k.) the offset matrices updating means is any structure which assigns new values in place of existing offset matrix entries, including the possibility of assigning values by use of another pseudo-random number generator or by selecting them from a list (page 8, lines 7-11, page 14, lines 8-10, and page 15, lines 18-21),

l.) the fifth application means is any structure which utilizes the matrix addition operation applying the updated offset matrices to the updated first intermediate matrices to create updated second intermediate matrix values (page 7, lines 2-6, page 14, lines 15-17),

m.) the modulus operator updating means is any structure which assigns new values in place of existing modulus operators, including the possibility of assigning values by use of another pseudo-random number generator or by selecting them from a list (page 9, lines 6-22, page 14, lines 10-12, and page 15, lines 21-24),

n.) the sixth application means is any structure which utilizes modular arithmetic and sequentially applies a set of updated modulus operators to the updated second intermediate matrices (page 7, lines 6-7, page 14, lines 17-20) to create values used to replace again the entries in the output matrices, and

o.) the updated output matrices second storage means is any structure, including a storage register, which stores updated values of the output matrix entries, (page 14, lines 5-6 and lines 13-15).

Thus, it is respectfully submitted that the means plus function language of claims 14 and 15 is supported by an adequate disclosure in the Specification showing what is meant by that language.

Section 102 Rejections

Claims 1 - 15 stand rejected under 35 U.S.C. 102(b) as being anticipated by Sriram. In essence, Sriram teaches a shifting process which repositions the output sequence of a linear feedback shift register (LFSR) pseudo-random number generator. The Sriram process uses binary matrix

multiplication of an initial state vector with sparse transitional matrices to shift in relative position within the entire sequence of the output results of a primary LFSR pseudo-random number generator. All sequential sets of results of Sriram's method will be subsets of the output results of the primary LFSR. Sriram's process generates and loops through all the possible sets of sequences of numbers generated by the primary LFSR, without generating any additional numbers which are not included in the original LFSR output.

In contrast, the claimed pseudo-random number generator uses general matrix multiplication of initial state matrices by fully-specified transitional matrices that are then incremented by fully-specified augmentation matrices against which a series of general modulus operators are applied to generate output state matrices from which pseudo-random numbers are extracted. It is highly unlikely that sequential sets of pseudo-random numbers generated by the claimed invention would match the results of any LFSR, since the period of the pseudo-random number sequence of the claimed invention would be significantly longer than the period of the sequence established by any comparable LFSR. Thus, the results of the claimed generator are entirely different than the results of Sriram's process.

Sriram does not apply a modulus operator as a part of its process, unlike the claimed invention. Sriram does mention modulo-2 multiplication in paragraphs 20 and 24, but that binary matrix multiplication serves only to produce a state matrix that is offset from the initial state matrix by an offset value. The claimed invention applies a modulus operator to an intermediate matrix to generate a new pseudo-random number matrix from which a pseudo-random number is extracted. Thus, the modulus operator of the claimed invention generates new matrix element entries from which a pseudo-random number is extracted, as opposed to shifting the position of an existing sequence of pseudo-random numbers as in Sriram.

Sriram's "offset state matrix" produces "a state matrix or vector that is offset or delayed from the initial state matrix by the offset value" (paragraph 20). There are no offset matrices in Sriram that are applied to an intermediate value to generate another value. The offset state matrix of Sriram is

simply an output matrix which is shifted in relative position within the sequence of the output results of the primary LFSR pseudo-random number generator.

The original claims of this application referred to offset matrices (now referred to as "augmentation matrices") which serve a very different purpose. Instead of shifting the position of output numbers, the offset matrices of this application are added to an intermediate matrix value to generate a second intermediate matrix value, which second intermediate matrix value most likely contains different element entries than those of the first intermediate matrix to which the offset matrix was applied. Thus, the offset matrices of the instant invention are more aptly called "augmentation matrices", since they serve to alter and augment element entries, rather than shifting the position of such numbers. To clarify this distinction from the offset state matrices of Sriram, the Specification is hereby amended to replace the defined term "offset matrix" with "augmentation matrix".

Therefore, the claimed invention differs from Sriram in three important and non-obvious ways:

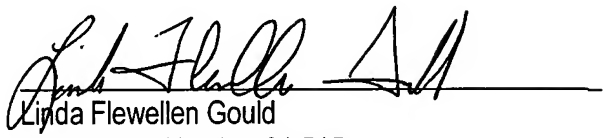
a.) Sriram teaches a shifting process which reorganizes the output of a LFSR, while the claimed invention generates significant numbers of values with no linear correlation or predictability, from which pseudo-random numbers are extracted,

b.) Sriram does not apply a modulus operator as a part of its process, while the claimed invention applies a modulus operator to generate new matrix element entries from which a pseudo-random number is extracted, and

c.) Sriram uses an offset state matrix to shift the relative position within a sequence of output results, which is not a part of the claimed invention. However, the claimed invention includes an augmentation matrix which alters and augments matrix element entries to create a significantly larger pool of numbers from which pseudo-random numbers are extracted.

In view of the above, it is submitted that the claims are in condition for allowance. Allowance of claims 1 - 15 at an early date is solicited.

Respectfully submitted,



Linda Flewellen Gould
Registration Number 31,515
Gould & Whitley
1665 Briargate Blvd., Suite 101
Colorado Springs, CO 80920
Telephone: (719) 531-0994
Fax: (719) 531-0996
Email: lgould@rwsoft.com

1. (Currently Amended) A method of generating a pseudo-random number, said method comprising the steps of:
   a. Establish initialization values for output series of pseudo-random number matrices $X_1 - X_k$;
   b. Store said initialized pseudo-random number matrices $X_1 - X_k$ in number matrices storage register;
   ~~b.~~c. Establish initialization values for variable transition matrices $A_{1,1} - A_{k,1}$;
   d. Store said initialized transition matrices $A_{1,1} - A_{k,1}$ in transition matrices storage register;
   ~~c.~~e. Establish initialization values for variable ~~offset~~ augmentation matrices $B_{1,1} - B_{j,1}$;
   f. Store said initialized augmentation matrices $B_{1,1} - B_{j,1}$ in augmentation matrices storage register;
   ~~d.~~g. Establish first modulus operators $m_{1,1} - m_{i,1}$;
   ~~e.~~h. Retrieve ~~Apply~~ said transition matrices $A_{1,1} - A_{k,1}$ and apply to said output series of pseudo-random number matrices $X_1 - X_k$ to generate a first intermediate matrix value $X_{firsttemp}$;
   ~~f.~~i. Retrieve ~~Apply~~ said ~~offset~~ augmentation matrices $B_{1,1} - B_{j,1}$ and apply to said first intermediate matrix value $X_{firsttemp}$ to generate a second intermediate matrix value X_{temp}; ~~and~~
   ~~g.~~j. Sequentially apply said first modulus operators $m_{1,1} - m_{i,1}$ to said second intermediate matrix value X_{temp} to generate an output value of pseudo-random number matrix X_n; ~~from which at least one pseudo-random number is extracted.~~
   k. Store said first output value matrix X_n in number matrices storage register;
   l. Retrieve and extract at least one pseudo-random number from element entries of said number matrices storage register; and
   m. Provide said pseudo-random number to long-term storage register for use in device which can employ pseudo-random numbers.

2. (Currently Amended) A method of generating a plurality of pseudo-random numbers, said method comprising the steps of:
   a. Establish initialization values for output series of pseudo-random number matrices $X_1 - X_k$;
   b. Store said initialized pseudo-random number matrices $X_1 - X_k$ in number matrices storage register;
   ~~b.~~c. Establish initialization values for variable transition matrices $A_{1,1} - A_{k,1}$;
   d. Store said initialized transition matrices $A_{1,1} - A_{k,1}$ in transition matrices storage register;
   ~~c.~~e. Establish initialization values for variable ~~offset~~augmentation matrices $B_{1,1} - B_{j,1}$;
   f. Store said initialized augmentation matrices $B_{1,1} - B_{j,1}$ in augmentation matrices storage register;
   ~~d.~~g. Establish first modulus operators $m_{1,1} - m_{i,1}$;
   ~~e.~~h. Retrieve ~~Apply~~ said transition matrices $A_{1,1} - A_{k,1}$ and apply to said output series of pseudo-random number matrices $X_1 - X_k$ to generate a first intermediate matrix value $X_{firsttemp}$;
   ~~f.~~i. Retrieve ~~Apply~~ said ~~offset~~augmentation matrices $B_{1,1} - B_{j,1}$ and apply to said first intermediate matrix value $X_{firsttemp}$ to generate a second intermediate matrix value X_{temp};
   ~~g.~~j. Sequentially apply said first modulus operators $m_{1,1} - m_{i,1}$ to said second intermediate matrix value X_{temp} to generate a first output value of pseudo-random number matrix X_n; ~~from which at least one pseudo-random number is extracted;~~
   ~~h.~~k. Store said first output value matrix X_n in ~~said~~ number matrices storage register to establish an updated output series of pseudo-random number matrices $X_{n-k+1} - X_n$;
   l. Retrieve and extract at least one pseudo-random number from element entries of said number matrices storage register;
   m. Provide each pseudo-random number to long-term storage register for use in device which can employ pseudo-random numbers;
   ~~i.~~n. Retrieve and u~~U~~pdate said transition matrices $A_{1,1} - A_{k,1}$ through updating process to create and store updated transition matrices $A_{1,2} - A_{k,2}$;
   ~~j.~~o. Retrieve ~~Apply~~ said updated transition matrices $A_{1,2} - A_{k,2}$ and apply to said updated output series of pseudo-random number matrices $X_{n-k+1} - X_n$ to generate an updated first intermediate matrix value $X_{firsttemp}$;

k.p. Retrieve and uUpdate said offsetaugmentation matrices $B_{1,1} - B_{j,1}$ through updating process to create and store updated offsetaugmentation matrices $B_{1,2} - B_{j,2}$;

l.q. Retrieve Apply said updated offsetaugmentation matrices $B_{1,2} - B_{j,2}$ and apply to said updated first intermediate matrix value $X_{firsttemp}$ to generate an updated second intermediate matrix value X_{temp};

m.r. Update said first modulus operators $m_{1,1} - m_{i,1}$ through updating process to create updated first modulus operators $m_{1,2} - m_{i,2}$;

n.s. Sequentially apply said updated first modulus operators $m_{1,2} - m_{i,2}$ to said updated second intermediate matrix value X_{temp} to generate a second output value of pseudo-random number matrix X_{n+1} from which at least one pseudo-random number is extracted; and

o.t. Store said second pseudo-random number matrix X_{n+1} in said number matrices storage register of pseudo-random number matrices.

3. (Currently Amended) A method of generating a plurality of pseudo-random numbers according to claim 2, wherein said steps i.l. through to. are repeated to generate a desired number d of pseudo-random number matrices X_{n+d} from which a plurality of element entries of said pseudo-random number matrices are extracted as pseudo-random numbers are extracted and provided to long-term storage register for use in device which can employ pseudo-random numbers.

4. (Original) A method according to claim 2 further comprising the step of:
Selecting a first subset of said pseudo-random numbers from said updated output series of pseudo-random number matrices.

5. (Original) A method according to claim 1, claim 2, or claim 3, wherein k = 1 so that a single variable transition matrix is used.

6. (Currently Amended) A method according to claim 1, claim 2, or claim 3, where j = 1 so that a single variable offsetaugmentation matrix is used.

7. (Original) A method according to claim 1, claim 2, or claim 3, where i = 1 so that a single modulus operator is used.

8. (Original) A method according to claim 2, further comprising the steps of:
a. Establish second modulus operators $r_{1,1} - r_{g,1}$;
b. Sequentially apply and update second modulus operators $r_{1,1} - r_{g,1}$, $r_{1,2} - r_{g,2}$, ... $r_{1,n+d-k} - r_{g,n+d-k}$ to said updated output series of pseudo-random number matrices to generate a second output series of pseudo-random number matrices.

9. (Currently Amended) A method according to claim 8, further comprising the step of:
Selecting a second subset of said pseudo-random numbers from element entries of said second output series of pseudo-random number matrices.

10. (Original) A method according to claim 1, claim 2, or claim 3:
a. Wherein said first modulus operators $m_{1,1} - m_{j,1}$, $m_{1,2} - m_{j,2}$, ... $m_{1,n+d-k} - m_{j,n+d-k}$ comprise a uniform variable modular reduction, and
b. Further comprising the step of discarding certain pseudo-random numbers which are not uniformly distributed.

11. (Original) A method according to claim 8:
a. Wherein said second modulus operators $r_{1,1} - r_{g,1}$, $r_{1,2} - r_{g,2}$, ... $r_{1,n+d-k} - r_{g,n+d-k}$ comprise a uniform variable modular reduction, and

b. Further comprising the step of discarding certain pseudo-random numbers which are not uniformly distributed.

12. (Currently Amended) A method according to claim 2 or claim 3, further comprising the steps of:

a. Create at least one ~~other~~ alternate storage register of pseudo-random number matrices by separately taking steps a – ~~to~~;

b. Create temporary composite pseudo-random number matrices by combining each resulting storage register of pseudo-random number matrices through at least one mathematical operation;

c. Create final composite pseudo-random number matrices by applying variable modular reduction to said temporary composite pseudo-random number matrices; and

d. Select a subset of pseudo-random numbers from element entries of said resulting final composite pseudo-random number matrices.

13. (Currently Amended) A method according to claim 1, claim 2, or claim 3 further comprising:

a. Apply an invertibility evaluation module to each second intermediate matrix value X_{temp};

b. Adjust ~~offset~~augmentation matrices $B_{1,1} - B_{j,1}$, $B_{1,2} - B_{j,2}$, ... $B_{1,n+d-1} - B_{j,n+d-1}$, so that said second intermediate matrix value X_{temp} is non-invertible;

c. Sequentially apply said first modulus operators $m_{1,1} - m_{i,1}$ to said non-invertible second intermediate matrix value X_{temp} to generate output value of non-invertible pseudo-random number matrix X_n from which at least one pseudo-random number is extracted; and

d. Select a subset of pseudo-random number output values from element entries of said non-invertible pseudo-random number matrices.

14. (Currently Amended) An apparatus for generating a pseudo-random number, said apparatus comprising:

a. Output matrices initialization means for establishing and storing initialization values for output series of pseudo-random number matrices $X_1 - X_k$ by assigning values to matrix entries;

b. Transition matrices initialization means for establishing and storing initialization values for variable transition matrices $A_{1,1} - A_{k,1}$ by assigning values to matrix entries;

c. ~~Offset~~ Augmentation matrices initialization means for establishing and storing initialization values for variable ~~offset~~augmentation matrices $B_{1,1} - B_{j,1}$ by assigning values to matrix entries;

d. Modulus operator initialization means for establishing first modulus operators $m_{1,1} - m_{i,1}$ by assigning values to modulus operators;

e. First application means for retrieving and applying said transition matrices $A_{1,1} - A_{k,1}$ to said output series of pseudo-random number matrices $X_1 - X_k$ to generate a first intermediate matrix value $X_{firsttemp}$;

f. Second application means for retrieving and applying said ~~offset~~augmentation matrices $B_{1,1} - B_{j,1}$ to said first intermediate matrix value $X_{firsttemp}$ to generate a second intermediate matrix value X_{temp}; and

g. Third application means for sequentially applying said first modulus operators $m_{1,1} - m_{i,1}$ to said second intermediate matrix value X_{temp} to generate and store an output value of pseudo-random number matrix X_n from element entries of which at least one pseudo-random number is extracted and provided to long-term storage for use in device which can employ pseudo-random numbers.

15. (Currently Amended) An apparatus for generating a plurality of pseudo-random numbers, said apparatus comprising:

a. Output matrices initialization means for establishing and storing initialization values for output series of pseudo-random number matrices $X_1 - X_k$ by assigning values to matrix entries;

b. Transition matrices initialization means for establishing and storing initialization values for variable transition matrices $A_{1,1} - A_{k,1}$ by assigning values to matrix entries;

c. ~~Offset~~ Augmentation matrices initialization means for establishing and storing initialization values for variable ~~offset~~augmentation matrices $B_{1,1} - B_{j,1}$ by assigning values to matrix entries;

d. Modulus operator initialization means for establishing first modulus operators $m_{1,1} - m_{i,1}$ by assigning values to modulus operators;

e.~~f.~~ First application means for retrieving and applying said transition matrices $A_{1,1} - A_{k,1}$ to said output series of pseudo-random number matrices $X_1 - X_k$ to generate a first intermediate matrix value $X_{firsttemp}$;

f.~~g.~~ Second application means for retrieving and applying said ~~offset~~augmentation matrices $B_{1,1} - B_{j,1}$ to said first intermediate matrix value $X_{firsttemp}$ to generate a second intermediate matrix value X_{temp};

g~~h~~. Third application means for sequentially applying said first modulus operators $m_{1,1} - m_{i,1}$ to said second intermediate matrix value X_{temp} to generate and store a first output value of pseudo-random number matrix X_n from element entries of which at least one pseudo-random number is extracted and provided to long-term storage for use in device which can employ pseudo-random numbers;

h~~i~~. Storage means for storing said first output value matrix X_n in a storage register to establish an updated output series of pseudo-random number matrices;

i~~j~~. Transition matrices updating means for retrieving and updating said transition matrices $A_{1,1} - A_{k,1}$ to create and store updated transition matrices $A_{1,2} - A_{k,2}$;

j~~k~~. Fourth application means for retrieving and applying said updated transition matrices $A_{1,2} - A_{k,2}$ to said updated output series of pseudo-random number matrices $X_{n-k+1} - X_n$ to generate an updated first intermediate matrix value $X_{firsttemp}$;

k~~l~~. ~~Offset~~ Augmentation matrices updating means for retrieving and updating said ~~offset~~augmentation matrices $B_{1,1} - B_{j,1}$ to create and store updated ~~offset~~augmentation matrices $B_{1,2} - B_{j,2}$;

l~~m~~. Fifth application means for retrieving and applying said updated ~~offset~~augmentation matrices $B_{1,2} - B_{j,2}$ to said updated first intermediate matrix value $X_{firsttemp}$ to generate an updated second intermediate matrix value X_{temp};

~~o.~~m~~n~~. Modulus operator updating means for updating said first modulus operators $m_{1,1} - m_{i,1}$ to create updated first modulus operators $m_{1,2} - m_{i,2}$;

n~~o~~. Sixth application means for sequentially applying said updated first modulus operators $m_{1,2} - m_{i,2}$ to said updated second intermediate matrix value X_{temp} to generate a second output value of pseudo-random number matrix X_{n+1} from element entries of which at least one pseudo-random number is extracted and provided to long-term storage register for use in device which can employ pseudo-random numbers; and

o~~p~~. Second storage means for storing said second pseudo-random number matrix X_{n+1} in said number matrices storage register ~~of pseudo-random number matrices~~.